

Appl. No. 09/385,589

Attorney Docket: 042390.P7574

**LISTING OF THE CLAIMS:**

This listing of claims replaces all prior versions, and listings, of claims in the application:

- 1 1. (Original) An apparatus comprising:  
2 at least one data bit generator to generate a first, second and third plurality of data bits;  
3 and  
4 a combiner function, coupled to the at least one data bit generator, including a network of  
5 shuffle units, to combine the third plurality of data bits, using the first and second plurality of  
6 data bits as first input data bits and control signals respectively of the network of shuffle units.
- 1 2. (Original) The apparatus of claim 1, wherein at least one of the shuffle units comprises a  
2 first and a second flip-flop to store a first and a second state value, and a plurality of selectors  
3 coupled to the first and second flip-flops in a topological manner to control selective output of  
4 one of the first and second state values based on a corresponding one of said second plurality of  
5 data bits.
- 1 3. (Original) The apparatus of claim 2, wherein said plurality of selectors are coupled to  
2 said first and second flip-flops of the shuffle unit in a topological manner that results in the first  
3 state value of the shuffle unit being output when the corresponding one of said second plurality  
4 of data bits is in a first state, and the second state value of the shuffle unit being output when the  
5 corresponding one of said second plurality of data bits is in a second state.
- 1 4. (Original) The apparatus of claim 2, wherein said plurality of the selectors are further  
2 coupled to said first and second flip-flops of the shuffle unit to control selective modification of

Appl. No. 09/385,589

Attorney Docket: 042390.P7574

3 the first and second state values stored in said first and second flip-flops of the shuffle unit based  
4 on the same corresponding one of said second plurality of data bits.

1 5. (Original) The apparatus of claim 4, wherein said plurality of selectors are coupled to  
2 said first and second flip-flops of the shuffle unit in a topological manner that results in the first  
3 state value being output and the first and second flip-flops of the shuffle unit to store said second  
4 state value and a second input data bit respectively when the corresponding one of said second  
5 plurality of data bits is in a first state, and the second state value being output and the first and  
6 second flip-flops of the shuffle unit to store the second input data bit and said first state value  
7 respectively when the corresponding one of said second plurality of data bits is in a second state.

1 6. (Original) The apparatus of claim 5, wherein the second input value is a selected one of  
2 an output data bit of an immediately preceding shuffle unit and an output data bit generated from  
3 said first plurality of data bits.

1 7. (Original) The apparatus of claim 1, wherein at least one of the shuffle units comprises a  
2 first and a second flip-flop to store a first and a second state value, and a plurality of selectors  
3 coupled to the first and second flip-flops to control modification of the first and second state  
4 values based on a corresponding one of said second plurality of data bits.

1 8. (Original) The apparatus of claim 7, wherein said plurality of selectors are coupled to the  
2 first and second flip-flops in a topological manner that results in the first and second flip-flops of  
3 the shuffle unit to store said second state value and a second input data bit respectively when the

Appl. No. 09/385,589

Attorney Docket: 042390.P7574

4 corresponding one of said second plurality of data bits is in a first state, and the first and second  
5 flip-flops of the shuffle unit to store the second input data bit and said first state value  
6 respectively when the corresponding one of said second plurality of data bits is in a second state.

1 9. (Original) The apparatus of claim 8, wherein the shuffle units are serially coupled to each  
2 other with a first of the shuffle unit serially coupled to the first XOR gate, and said second input  
3 data bit is a selected one of an output bit of an immediately preceding shuffle unit and an output  
4 bit generated from the first plurality of data bits.

1 10. (Original) The apparatus of claim 1, wherein the combiner function further comprises an  
2 exclusive-OR gate to combine the first plurality of data bits for the network of shuffle units.

1 11. (Original) The apparatus of claim 1, wherein the combiner function further comprises an  
2 exclusive-OR gate to combine the third plurality of data bits using an output bit of the network of  
3 shuffle units.

1 12. (Original) The apparatus of claim 11, wherein the apparatus further comprises a register  
2 coupled to the XOR gate to store a cipher key and allow the stored cipher key to be periodically  
3 modified by the output of the exclusive-OR gate.

1 13. (Original) The apparatus of claim 12, wherein the apparatus further comprises a function  
2 block coupled to the register to successively transform the modified cipher key, and a mapping

Appl. No. 09/385,589

Attorney Docket: 042390.P7574

3 block coupled to the register to generate a pseudo random bit sequence based on the successive  
4 transformed states of the modified random number.

1 14. (Original) The apparatus of claim 1, wherein the at least one data bit generator comprises  
2 a plurality of LFSRs to generate said first, second, and third plurality of data bits.

1 15. (Original) The apparatus of claim 1, wherein the apparatus is a stream cipher.

1 16. (Cancelled).

1 17. (Previously Presented) An apparatus comprising:  
2 a first XOR gate to receive a first plurality of data bits and combine them into a second  
3 data bit;  
4 a network of shuffle units, coupled to the first XOR gate, to output a third data bit by  
5 shuffling and propagating the second data bit through the network of shuffle units under the  
6 control of a fourth plurality of data bits; and  
7 a second XOR gate coupled to the network of shuffle units to combine a fifth plurality of  
8 data bits using the third data bit;  
9 wherein at least one of the shuffle units comprises a first and a second flip-flop to store a  
10 first and a second state value, and a plurality of selectors coupled to the first and second flip-  
11 flops to control selective output of one of the first and second state values based on a  
12 corresponding one of said fourth plurality of data bits.

Appl. No. 09/385,589

Attorney Docket: 042390.P7574

1 18. (Previously Presented) The apparatus of claim 17, wherein said plurality of selectors are  
2 coupled to the first and second flip-flops of the shuffle unit in a topological manner that results in  
3 the first state value of the shuffle unit being output when the corresponding one of said fourth  
4 plurality of data bits is in a first state, and the second state value of the shuffle unit being output  
5 when the corresponding one of said fourth plurality of data bits is in a second state.

1 19. (Previously Presented) The apparatus of claim 18, wherein said plurality of the selectors  
2 are further coupled to the first and second flip-flops to control selective modification of the first  
3 and second state values stored in the first and second flip-flops of the shuffle unit based on the  
4 same corresponding one of said fourth plurality of data bits.

1 20. (Previously Presented) The apparatus of claim 19, wherein said plurality of selectors are  
2 coupled to the first and second flip-flops of the shuffle unit in a topological manner that results in  
3 the first state value being output and the first and second flip-flops of the shuffle unit to store  
4 said second state value and a sixth data bit respectively when the corresponding one of said  
5 fourth plurality of data bits is in a first state, and the second state value being output and the first  
6 and second flip-flops of the shuffle unit to store the sixth data bit and said first state value  
7 respectively when the corresponding one of said fourth plurality of data bits is in a second state.

1 21. (Previously Presented) The apparatus of claim 20, wherein the shuffle units are serially  
2 coupled to each other with a first of the shuffle unit serially coupled to the first XOR gate, and  
3 said sixth data bit is a selected one of said second data bit and the output of an immediately  
4 preceding shuffle unit.

Appl. No. 09/385,589

Attorney Docket: 042390.P7574

1 22. (Previously Presented) The apparatus of claim 17, wherein at least one of the shuffle  
2 units comprises a first and a second flip-flop to store a first and a second state value, and a  
3 plurality of selectors coupled to the first and second flip-flops to control modification of the first  
4 and second state values based on a corresponding one of said fourth plurality of data bits.

1 23. (Previously Presented) The apparatus of claim 22, wherein said plurality of selectors are  
2 coupled to the first and second flip-flops of the shuffle unit in a topological manner that results in  
3 the first and second flip-flops of the shuffle unit to store said second state value and a sixth data  
4 bit respectively when the corresponding one of said fourth plurality of data bits is in a first state,  
5 and the first and second flip-flops of the shuffle unit to store the sixth data bit and said first state  
6 value respectively when the corresponding one of said fourth plurality of data bits is in a second  
7 state.

1 24. (Previously Presented) The apparatus of claim 23, wherein the shuffle units are serially  
2 coupled to each other with a first of the shuffle unit serially coupled to the first XOR gate, and  
3 said sixth data bit is a selected one of said second data bit and the output of an immediately  
4 preceding shuffle unit.

1 25. (Previously Presented) The apparatus of claim 17, wherein the apparatus further  
2 comprises a register coupled to the second exclusive-OR gate to store a value to be periodically  
3 modified using the result of said combination of the fifth plurality of data bits.

Appl. No. 09/385,589

Attorney Docket: 042390.P7574

1 26. (Previously Presented) The apparatus of claim 25, wherein the apparatus further  
2 comprises a function block coupled to the register to successively transform a modified version  
3 of the stored value, and a mapping block coupled to register to generate a pseudo random bit  
4 sequence based on the successively transformed states of the modified value.

1 27. (Previously Presented) The apparatus of claim 26, wherein the apparatus is a stream  
2 cipher.

1 28. (Previously Presented) A hardware implemented method using a network of shuffle units  
2 comprising:  
3 generating a first, second and third plurality of data bits; and  
4 shuffling and propagating a fourth data bit generated from the first plurality of data bits,  
5 under the control of the second plurality of data bits, to output a fifth data bit to combine the  
6 third plurality of data bits.

1 29. (Previously Presented) The method of claim 28, wherein the fourth data bit is serially  
2 shuffle and propagated, and at each stage, a first state value is output when the corresponding  
3 one of said second plurality of data bits is in a first state, and a second state value is output when  
4 the corresponding one of said second plurality of data bits is in a second state.

1 30. (Previously Presented) The method of claim 28, wherein the fourth data bit is serially  
2 shuffle and propagated, and at each stage, a first of the state values is replaced by an input value,  
3 and shuffled, when the corresponding one of said second plurality of data bits is in a first state,

Appl. No. 09/385,589

Attorney Docket: 042390.P7574

- 4 and a second of the state values is replaced by the input value, and shuffled, when the
- 5 corresponding one of said second plurality of data bits is in a second state.